On Bases of Finite Fields for Cryptography

by

DHIRENDRA SINGH YADAV

Department of Mathematics

submitted
in fulfillment of the requirements
of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi
November 2011

CERTIFICATE

This is to certify that the thesis entitled *"On Bases of Finite Fields for Cryptography"* submitted by *Mr. Dhirendra Singh Yadav* to the Indian Institute of Technology Delhi, for the award of the Degree of Doctor of Philosophy, is a record of the original bona fide research work carried out by him under our guidance and supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Prof. R. K. Sharma
(Supervisor)

Dr. Wagish Shukla
(Supervisor)

November 2011
Department of Mathematics
Indian Institute of Technology Delhi

Acknowledgements

First and foremost, I offer my sincerest gratitude to my supervisors Prof. R. K. Sharma and Dr. Wagish Shukla, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject. They have supported me throughout my thesis with their patience and knowledge whilst allowing me the room to work in my own way. Without them this thesis would not have been completed or written.

I would like to express my deep sense of gratitude to Prof. Suresh Chandra and Prof. J. B. Srivastava for providing me unflinching encouragement and support in various ways. I am privileged to have the opportunity to come in contact with them for academic discussions.

I am thankful to IIT Delhi authorities for providing me the necessary facilities for smooth completion of my work. I would like to extend my appreciation to my SRC (Student Research Committee) members Dr. Aparna Mehra and Prof. S. K. Gupta (Department of Computer Science and Engineering, IIT Delhi), as well as to all the faculty members of the Department of Mathematics, IIT Delhi for their encouragement. I would also like to thank CSIR for providing financial assistance by awarding me a research fellowship during my research work.

I would like to thank all my friends and colleagues for their constant encouragement and support. I would particularly like to thank Dhiman, Suyash, Pratap,

Mradul, Rajendra Uppal, Puneet, Balchand, Pooja, Sunil, Dinbandhu, Anand, Alok, Varun, Anubha, Neha, Ankita, Deep Chandra, Resham, Varsha, Sarvesh, Vandana, Bhavya, Arti Singh, Arti Pandey, Arti Sengar, Amit, Megha, Reshma, and S. Ramasamy for being there to share the various highs and lows, lunch and dinner and numerous cups of coffee at the coffee shop. I appreciate all my seniors for making me comfortable in the department and, motivating in the initial days of my research.

My deepest gratitude goes to my family for their unflagging love and support throughout my life; without them this dissertation is simply impossible.

Finally, I thank the almighty God for his blessings.

New Delhi Dhirendra Singh Yadav

November 2011

Abstract

Finite fields are becoming increasingly important for cryptography. Among the more common finite fields in cryptography are odd-characteristic finite fields $\mathbb{F}_p$ and even characteristic finite fields $\mathbb{F}_{2^m}$. Arithmetic in any finite field can be further classified according to the choice of basis for representing elements of the finite field. A good choice of a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is a very important circumstance which facilitates computation in finite fields. The aim of this thesis is a systematic and focussed study of various types of bases of finite fields and their cryptographic significance. Representation and arithmetic of finite fields with respect to different bases and their suitability for various cryptographic applications have been discussed. Our contributions include a new proof of the homogenous property of trace map. It is a constructive proof and provides exact information about affine subspaces consisting of equal trace elements. We have proved an explicit formula to associate a given linear functional on $\mathbb{F}_{q^m}$ to a unique element of $\mathbb{F}_{q^m}$ as a unique root of m affine polynomial defined by the linear functional and a fixed basis. This explicit formula may further lead to some constructive results which earlier were only existential in nature. Our contribution also include some results on reducibility and irreducibility of polynomials over prime fields. We have also proposed a key exchange scheme that makes use of singular matrices over finite fields to transfer data over insecure channels.

Notations

In the following notations A is a set, I is an ideal, and R is a ring.

Notation/Symbol	**Meaning**
$\mathbb{N}$	set of natural numbers
$\mathbb{Z}$	set of integers
$\mathbb{Q}$	set of rational numbers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\lfloor x \rfloor$	greatest integer less than or equal to x
$\Leftrightarrow$	implies and is implied by
$[a, b]$	set of all integers x such that $a \leq x \leq b$
$Ord_n(a)$	order of a modulo n
$Ord(a)$ or $\lvert a \rvert$	order of element a in a group
$\equiv$	is congruent to
$\phi(\cdot)$	Euler's phi function
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\lvert A \rvert$	number of elements in the set A
$R[x]$	ring of polynomials over ring R and indeterminate x
$\mathbb{F}_q$	finite field with q elements
$\mathbb{F}_q^*$	set of all non-zero elements of finite field $\mathbb{F}_q$
$\mathbb{F}_q(\alpha)$	smallest field containing α and field $\mathbb{F}_q$
$\in$	belongs to
$\notin$	does not belong to
$\subseteq$	subset or equal
$\subsetneq$	proper subset
$A \backslash B$	difference of sets A and B
$\cup, \cap$	union, intersection
$\lvert X \rvert$	cardinality of set X
$\emptyset$	empty set

$\cong$	is isomorphic to
$\|R : I\|$	index of I in R
R/I	quotient of R by I
$[F : K]$	degree of F over K
$M_n(R)$	ring of $n \times n$ matrices over R
$GL(n, R)$	general linear group of $n \times n$ matrices over R
$SL(n, R)$	special linear group of $n \times n$ matrices over R
$sd(m, q)$	number of self-dual bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$
$N_q(m)$	number of polynomial bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$

Contents

Acknowledgements iii

Abstract v

Notations vii

1 Introduction 1

2 Prerequisites 7

2.1 Groups, Rings and Polynomials 7

2.2 Vector Spaces and Finite Fields 11

2.2.1 Bases and Linear Transformations 11

2.2.2 Roots of Polynomials and Splitting Fields 14

2.2.3 Characterization of Finite Fields 16

2.2.4 Bases of Finite Fields 18

2.2.5 Roots of Unity and Affine Polynomials 20

3 Polynomial Bases 23

3.1 Introduction 23

3.1.1 Number of Polynomial Bases 25

3.2 Irreducible Polynomials over Finite Fields 28

3.3 Operations over $\mathbb{F}_{2^m}$ 34
3.3.1 Multiplication 34
3.3.2 Exponentiation 39
3.3.3 Inversion and Division 39
3.4 Trinomials, Pentanomials, and OEF 40
3.5 Polynomial Bases and Cryptography 41

4 Dual and Self-dual Bases **43**
4.1 Trace Map and Duality 43
4.1.1 Number of Self-dual Bases 57
4.2 Dual Basis and Bit-Serial Multipliers 59

5 Normal and Optimal Normal Bases **61**
5.1 Normal Bases 61
5.1.1 Properties of Normal Bases 63
5.2 Optimal Normal Bases 65
5.2.1 Existence of Optimal Normal Bases 69
5.3 Arithmetic of $\mathbb{F}_{2^m}$ using Normal Basis 72
5.3.1 Addition/Subtraction 72
5.3.2 Multiplication 72
5.3.3 Squaring/Exponentiation 74
5.3.4 Inversion/Division 75
5.4 Normal Bases and Cryptography 76

6 Applications in Cryptography **77**
6.1 Bases of Finite Fields and Cryptosystems 77
6.1.1 Hidden Monomial Cryptosystem 78
6.1.2 Double-Round Quadratic Enciphering 81
6.2 Use of Singular Matrices in Cryptography 83

7 Conclusion **89**

7.1 Summary of the Thesis 89

7.2 Future Work 90

A Integers and Divisibility **93**

B Algorithms **101**

Bibliography **107**

Index **115**

Bio-data **121**